Algunas aplicaciones de los esquemas de asociación mediante bases de Gröbner.[1]

Edgar Martínez-Moro

Dpto. de Matemática Aplicada Fundamental
Universidad de Valladolid.
e-mail: edgar.martinez@ieee.org

Resumen

En esta comunicación mostramos algunas nuevas aplicaciones del tratamiento de la estructura del álgebra de Bose-Mesner de un esquema de asociación conmutativo mediante bases de Gröbner.

1 Introducción

En esta comunicación mostramos cómo algunos resultados sobre la estructura de los esquemas de asociación, en concreto de su álgebra de Bose-Mesner, pueden ayudarnos a replantear algunos problemas de la matemática aplicada. Algunas de las técnicas que se muestran en esta comunicación han sido utilizadas el la teoría de la codificación algebraica [8, 9, 10, 11]. Un enfoque mas general se puede encontrar en [12].

La estructura de la comunicación es la siguiente: En la primera sección expondremos de manera breve el concepto de esquema de asociación, para un estudio completo de los mismos ver, por ejemplo, [1]. En la sección segunda se aborda el estudio del álgebra de Bose-Mesner $\mathcal{B}$ de un esquemas de asociación desde un punto de vista de la bases de Gröbner [8, 9, 10]. Para aquellos lectores no familiarizados con las bases de Gröbner una buena introducción es el texto [2], un resumen conciso del material utilizado se encuentra como apéndice en [10]. Finalmente en la sección tercera se muestran dos aplicaciones del algoritmo propuesto que encuentra una matriz generadora para el álgebra $\mathcal{B}$ en la sección 2.

[1]Trabajo parcialmente subvencionado por la Junta de Castilla y León y MCyT (BFM2001-22)

2 Estructura de los esquemas de asociación

En esta sección exponemos la construcción del álgebra de Bose-Mesner de un esquema de asociación, así como algunas de sus propiedades. Este material y sus demostraciones pueden ser encontradas en [8, 10].

Definición 1 *Llamaremos* **esquema de asociación**[1] *S, a una familia de $m+1$ matrices simétricas de orden n $(A_i)_{i=0}^m$ con entradas en $\{0,1\}$ tales que:*

a) $\sum_{i=0}^m A_i = J$,

b) $A_0 = I_n$,

c) $\exists p_{ij}^k$, $0 \leq i,j,k \leq m$ *constantes, tal que* $A_iA_j = \sum_{k=0}^m p_{ij}^k A_k$

Donde J es la matriz con todas sus entradas 1 e I_n es la matriz identidad de orden n. Por las condiciones anteriores, $\{A_i\}_{i=0}^m$ es una base (como C-espacio vectorial) del un subálgebra conmutativa de $M_n(C)$ con dimensión $m+1$ que denotaremos por $\mathcal{B}$. Se suele denominar a $\mathcal{B}$ álgebra de *Bose-Mesner* del esquema de asociación. Los esquemas de asociación pueden formularse en un ámbito más general como relaciones entre elementos de un conjunto y son unas estructuras importantes en teoría de diseños y teoría de códigos [1, 3].

De la condición c) se sigue $\{A_i\}_{i=0}^m$ forman una familia de matrices que conmutan, y por lo

[1]En la mayoría de las referencias sobre esquemas de asociación, esta definición corresponde a esquema de asociación conmutativo.

tanto son simultáneamente diagonalizables. Esto es, podemos encontrar una base de idempotentes $\{E_i\}_{i=0}^m$ de $\mathcal{B}$ tal que:

a') $\sum_{i=0}^m E_i = I_n$,

b') $E_0 = \frac{1}{n}J$,

c') $E_iE_j = \delta_{ij}E_i$.

La matriz de cambio de base entre las base de las matrices de adjacencia y la base de idempotentes se llama *tabla de caracteres* y la denotaremos por:

$$P = [p_i(j)]_{i,j=0}^m$$

y sus entradas se denominan *primeros autovalores* del esquema de asociación.

3 Bases de Gröbner y esquemas de asociación

La obtención de una base de Gröbner para el álgebra de Bose-Mesner del esquema de asociación viene se deriva del siguiente hecho: *los primeros autovalores del esquema de la definición 1 son las soluciones no nulas del sistema de ecuaciones siguiente (ver [8] para una demostración completa)*:

$$x_ix_j - \sum_{k=0}^m p_{ij}^k x_k = 0 \quad 0 \le i \le j \le m \qquad (1)$$

Consideremos el siguiente conjunto del polinomios:

$$\mathcal{F} = \left\{x_ix_j - p_{ij}^0 - \sum_{k=1}^m p_{ij}^k x_k\right\}_{1\le i\le j\le m} \bigcup \left\{x_0 - 1\right\} \qquad (2)$$

que denominaremos **polinomios estructurales**. Sea $\mathcal{I} = \langle\mathcal{F}\rangle$ el ideal generado por $\mathcal{F} \subseteq C[x_0,\ldots,x_m]$. Este ideal $\mathcal{I}$ tiene las siguientes propiedades:

- $\mathcal{F}$ es una *base de Gröbner reducida* del ideal $\langle\mathcal{F}\rangle = \mathcal{I}$ para el orden monomial dado por el grado total. La comprobación de este hecho es inmediata, ya que los términos líderes del los polinomios en la base generan el ideal generado por los términos líderes de $\mathcal{I}$.
- La variedad $V(\mathcal{I})$ (i.e. las soluciones no nulas de las ecuaciones en (1)) es cero-dimensional, i.e. está formada por un número finito de puntos.
- La forma normal para el producto x_ix_j es:

$$nf(x_ix_j) = x_ix_j - [x_ix_j - p_{ij}^0 - \sum_{k=1}^m p_{ij}^k x_k] \qquad (3)$$

$$= p_{ij}^0 + \sum_{k=1}^m p_{ij}^k x_k \quad 1 \le i \le j \le m$$

  Por lo tanto, las matrices de multiplicación $M^i, 0 \le i \le d$ del álgebra de Bose-Mesner vienen dadas por:

$$M^i = \left(m_{ld}^i\right)_{l,d=0}^m, \quad \text{where } m_{ld}^i = p_{li}^d \qquad (4)$$

  Estas matrices se conocen como *matrices de intersección* y generan un álgebra sobre C isomorfa a $\mathcal{B}$ denominada *álgebra de intersección.* Resolver las ecuaciones en (1) es lo mismo que diagonalizar el álgebra de intersección (ver [8]), y por lo tanto $\mathcal{B}$.
- $\mathcal{I}$ es un ideal radical. Como $\mathcal{B}$ es conmutativa y semisimple no contiene elementos nilpotentes. Pero los elementos en $\sqrt{\mathcal{I}} \setminus \mathcal{I}$ corresponden a los elementos nilpotentes del álgebra, por lo tanto $\mathcal{I}$ es un ideal radical.

Las observaciones anteriores permiten traducir propiedades combinatorias del álgebra de Bose-Mesner en términos de propiedades del ideal $\mathcal{I}$. Nótese además que los cálculos sobre el ideal $\mathcal{I}$ pueden ser realizados de forma eficiente sin necesidad de utilizar el algoritmo original del Buchberger para calcular la base (que en general no es eficiente). Por el contrario, al ser nuestro ideal cero-dimensional y radical, y tener garantizada a priori una base de Gröbner nos permite calcular por medio de técnicas FGLM [4] (o de reordenamiento) otras bases con respecto otros órdenes monomiales. Estas técnicas se pueden establecer en términos de álgebra lineal. En este sentido en [9, 10] se muestra cómo determinar si el esquema es P-polinomial o cómo calcular los polinomios de Lloyd del esquema.

En esta comunicación mostramos un algoritmo que nos permite encontrar una matriz $A \in \mathcal{B}$ cuyas entradas son enteros no negativos tal que

todo elemento del álgebra de Bose-Mesner se expresa como un polinomio en A, esto es, genera todo el álgebra $\mathcal{B}$.

Diremos que un ideal $\mathcal{I} \subset C[x_0, \ldots, x_m]$ está en *posición genérica* respecto a m si para cada par $(a_0^1, \ldots, a_m^i) \in V(\mathcal{I})$, $i = 1, 2$ se tiene $a_n^1 \neq a_n^2$.

Lema 2 *Una combinación lineal $A = \sum_{i=0}^{m} \lambda_i D_i$ de matrices de adyacencia del esquema genera el álgebra $\mathcal{B}$ si y sólo si el ideal $\mathcal{I}$ está en posición genérica con respecto a un cambio de variables en que $y_n = \sum_{i=0}^{m} \lambda_i x_i$.*

Una modificación del algoritmo 5.4 en [5] nos permite encontrar dicho elemento $A \in \mathcal{B}$. La idea subyacente en el mismo es realizar cambios aleatorios de coordenadas hasta que el ideal se encuentre en posición genérica.

Algoritmo 1 (Calcula A)

- **Input** $\mathcal{F}$ *Ecuaciones estructurales de* $\mathcal{S}$,
- **Calcula** *una base de Gröbner reducida* $\mathcal{G}$ *de* $\langle \mathcal{F} \rangle$ *para un orden monomial plex. con* $x_m < x_j$ $0 \leq j < m$
- **Repetir**
  Sea $\langle g \rangle = \mathcal{G} \cap R[x_m]$.
  Sea i *el mayor índice tal que para cada* $j \leq i$, x_j *se puede expresar como un polinomio en* x_m.
  Si $i < m - 1$ *entonces*
  Elije *un entero positivo* c *aleatorio*
  Calcula *el cambio de coordenadas:*

$$\begin{aligned} x_j &\mapsto x_j \quad 0 \leq j < m \\ cx_i + x_m &\mapsto x_m \end{aligned} \tag{5}$$

  Calcula *una base de Gröbner reducida* $\mathcal{G}$ *con el mismo ordenamiento en las nuevas variables.*
  Hasta $i = m - 1$ **Stop**
- **Output** *La base de Gröbner y el cambio de coordenadas que obtuvo el último* x_m.

Los lectores interesados en el algoritmo pueden consultar el artículo [5].

Ejemplo 1 *Sea $X = Z_s, s, r \in N$ y $r < m$. Consideremos el subgrupo de Z_s^* generado por r y -1; Éste actúa sobre X, con órbitas $\mathcal{O}_k$. Las siguientes relaciones definen un esquema de asociación sobre X:*

$$xR_k y \Leftrightarrow x - y \in \mathcal{O}_k$$

Si $s = 31, r = 2$ las órbitas son: $\mathcal{O}_0 = \{0\}$, $\mathcal{O}_1 = \{\pm 1, \pm 3\}$, $\mathcal{O}_2 = \{\pm 2, \}$, $\mathcal{O}_3 = \{4\}$ El ideal $\mathcal{I}$ está generado por:

$$\begin{aligned} &\{{x_1}^2 - 4\,x_2 - 4\,x_3 - 4, \\ &{x_3}^2 - 1,\, x_0 - 1,\, x_1\,x_2 - 2\,x_1, \\ &x_1\,x_3 - x_1,\, {x_2}^2 - 2\,x_3 - 2,\, x_2\,x_3 - x_2\} \end{aligned} \tag{6}$$

Si realizamos el cambio de coordenadas:

$$\begin{aligned} x_i &\mapsto y_i \quad 0 \leq i < 3 \\ x_3 + x_1 &\mapsto y_3 \end{aligned}$$

Las ecuaciones (6) se transforman en:

$$\begin{gathered} y_1^2 - 4y_2 - 4(y_3 - y_1) - 4,\, (y_3 - y_1)^2 - 1, \\ y_0 - 1,\, y_1 y_2 - 2y_1,\, y_1(y_3 - y_1) - y_1, \\ y_2^2 - 2(y_3 - y_1) - 2,\, y_2(y_3 - y_1) - y_2 \end{gathered}$$

Considerando el orden plex. $y_3 < y_1, y_2$ obtenemos la base Gröbner :

$$\begin{gathered} 12y_1 - y_3^3 + 3y_3^2 + y_3 - 3, \\ 27 + 24y_2 - 3y_3^2 + 25y_3 - y_3^3, \\ 15 - 16y_3^2 + 2y_3 - 2y_3^3 + y_3^4,\, y_0 - 1 \end{gathered}$$

Por lo tanto el ideal se encuentra en posición genérica y el álgebra de Bose-Mesner se puede expresar en terminos de la matriz $A = D_1 + D_3$.

4 Aplicaciones

Finalmente mostramos dos aplicaciones de las técnicas y conceptos de las anteriores secciones. No mostraremos las dedicadas a los esquemas definidos para las métricas usadas en códigos correctores por estar recogidas en [8, 9, 10]. Mostraremos sin embargo, su aplicación a otros dos problemas:

4.1 Cálculo de la complejidad de comunicación

Sean $(A_i)_{i=0}^m$ las matrices de adyacencia de un esquema de asociación. Una combinación lineal $\sum_{k=0}^{m} c_k D_k$ puede ser considerada como la matriz $(f(x,y))_{x,y}$, que representa la función donde $f(x,y) = c_k$ si (x,y) es un elemento de la relación

D_k. Uno de los parámetro básicos a conocer de estas matrices [13] es su *complejidad de comunicación* $C(f)$, que es el número mínimo de bits que dos personas tienen que intercambiar para evaluar $f(x,y)$ si una persona conoce inicialmente x y la otra y. Esta característica es importante a la hora de diseñar circuitos VLSI. En [13] se muestra como dicha complejidad $C(f)$ depende de que los autovalores de la matriz $(f(x,y))$ difieran de 0 o no, sin duda para esta comprobación podemos utilizar el algoritmo anterior. [2]

4.2 Programas semidefinidos sobre esquemas de asociación

Este enfoque ha sido abordado ya por Goemans-Rendl [7], sin embargo su método supone la diagonalización de todas las matrices de adyacencia del esquema de asociación. Nosotros utilizamos el hecho de que el álgebra de Bose-Mesner siempre está generada por una sóla matriz A. Dicha matriz, así como la expresión de las matrices de adyacencia en función de ella se pueden calcular por el algoritmo anterior.

Los *programas semidefinidos* (PS) son una herramienta fundamental en muchos campos de la matemática aplicada, especialmente en optimización combinatoria. Un importante "survey"sobre los principales resultados sobre PS y sus aplicaciones puede encontrarse en [14]. Consideramos el problema PS dado para un conjunto de matrices simétricas $F_i, \quad i = 0, \ldots m$ por:

$$\begin{array}{ll} \text{Maximizar} & \mathbf{Tr} F_0 \cdot Z \\ \text{Sujeto a} & \mathbf{Tr} F_i \cdot Z = c_i, \quad i = 1, \ldots, m \\ & Z \tilde{>} 0. \end{array} \tag{7}$$

Donde $\tilde{>}$ significa que X sea semidefinida positiva. El programa *dual* (PS-D) puede ser entendido como minimizar una función lineal sujeta a la condición de que una combinación afín de matrices simétricas sea definida positiva, es decir:

$$\begin{array}{ll} \text{Minimizar} & c^t \cdot x \\ \text{Sujeto a} & F(x) \tilde{>} 0 \\ & F(x) = F_0 + \sum_{i=1}^{m} x_i F_i. \end{array} \tag{8}$$

[2] En esquemas de asociación métricos la complejidad de comunicación se puede calcular a partir de los polinomios de Lloyd, estos pueden ser calculados también mediante bases de Gröbner, ver [10].

En el caso en que las matrices $\{F_0, \ldots, F_m\}$ se encuentren en el álgebra de Bose-Mesner de un esquema de asociación, nótese que la matriz

$$Z = \sum_{j \geq 1} y_j F_j - F_0$$

tambien pertenece al esquema de asociación. La observación clave es que, dado que podemos encontrar una matriz A que genera el álgebra, los autovalores de las matrices $F_j \quad j \geq 1$ y de F_0 son conocidos (pues $F_i = p_i(A)$ donde P es un polinomio). Por tanto, $Z \tilde{>} 0$ si $My \geq c$, donde M es una matriz que recoge los autovalores de $F_j \quad j \geq 1$ y c es el vector columna que recoge los autovalores de F_0. Por lo tanto el problema (PS-D) se transforma en un problema de progamación lineal.

Referencias

[1] Bannai, E.; Ito, T. *Algebraic combinatorics I: association schemes.* The Benjamin/Cummings Publishing Co., Inc., Menlo Park, CA, 1984.

[2] Cox, D.; Little,J.; O'Shea, D. *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra.* Second edition. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1997.

[3] Delsarte, P.; Levenshtein, V. I. Association schemes and coding theory. Information theory: 1948–1998. IEEE Trans. Inform. Theory 44 (1998), no. 6, 2477–2504.

[4] Faugère, J.; Gianni,P.; Lazard, D.; Mora, T. *Efficient computation of zero-dimensional Grbner bases by change of ordering.* J. Symbolic Comput. 16 (1993), no. 4, 329–344.

[5] Gianni, P.; Mora; T. *Algebraic solution of systems of polynomial equations using Gröbner bases.*, Applied algebra, algebraic algorithms and error-correcting codes (Menorca, 1987), 247–257, Lecture Notes in Comput. Sci., 356, Springer, Berlin, 1989.

[6] Gianni, P.; Trager, B.; Zacharias, G. *Gröbner bases and primary decomposition of polyno-*

mial ideals. Computational aspects of commutative algebra. J. Symbolic Comput. 6 (1988), no. 2-3, 149–167.

[7] M. X. Goemans and F. Rendl. Semidefinite programs and association schemes. *Computing*, 63(4):331–340, 1999.

[8] E. Martínez-Moro. Computations on character tables of association schemes. In *Computer algebra in scientific computing—CASC'99 (Munich)*, pages 293–307. Springer, Berlin, 1999.

[9] E. Martínez-Moro. *Estructura combinatoria de métricas no-Hamming.* Tesis, Universidad de Valladolid, 2001.

[10] E. Martínez-Moro. Properties of commutative association schemes derived by FGLM techniques. *Int. Journal of Algebra and Computation*, To appear in Dec. 2002. 20pp.

[11] E. Martínez-Moro. *Gröbner basis and association schemes: some applications.* Invited conference at the special session on coding at MSCIT 2002. Galway, Jul. 2002.

[12] E. Martínez-Moro. *Regular Representations of Finite-dimensional Separable Semisimple Algebras and Gröbner.* Preprint, submitted to Int. Journal of Symbolic Computation in Aug. 2002.

[13] U. Tamm Communication complexity and orthogonal polynomials. *DIMACS series on Discrete Mathematics*, 56, 277–285.

[14] L. Vandenberghe and S. Boyd. Semidefinite programming. *SIAM Rev.*, 38(1):49–95, 1996.